UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,127	01/17/2001	John R. Hind	RSW920010010US1	6523

7590	07/12/2005

Jeanine S. Ray-Yarletts
IBM Corporation T81/503
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER
JACKSON, JAKIEDA R

ART UNIT	PAPER NUMBER
2655	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
	09/765,127	HIND ET AL.
Office Action Summary	Examiner	Art Unit	
	Jakieda R Jackson	2655	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>25 April 2005</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-10,12-34,36-58 and 60-72</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-10,12-34,36-58 and 60-72</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>4/25/05</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   In response to the Office Action mailed January 25, 2005, applicant submitted an

amendment filed on April 25, 2005, in which the applicant traversed and requested

reconsideration with respect to amended independent **claims 1, 25 and 49**.

Response to Arguments

2.   Applicants argue that the cited references taken alone or in combination, fail to

teach or suggest at least a security core that is configured to abort the recording and the

transforming if one or more of the audio recording component and the at least one

transformation component fails to remain operably connected to the security core during

the recording of the audio stream and the transforming of the audio stream. In

particular, applicant argues that Cooper discuses that "an expert or consultant may

decide to either not archive any portion of the session or to abort the archiving process

because of potential liability problems, whereas the amended claim 1 now recites that

the security core does the aborting, when a condition is met. Applicant further argues

that Cooper proposes allowing the user discretion to abort a process, which teaches

away from a security core that is configured to abort the process, as amended.

Applicant's arguments with respect to claims 1, 25 and 49 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Objections

3.   Claims 6-8, 15, 21 and 31 are objected to because of the following informalities:

-   Regarding claims 6-8, lines 1-2 "wherein the the", should be --wherein the--.

-   Regarding claim 15, lines 1-2 "according to claim 1, the security core", should be
    --according to claim 1, wherein the security core--.

-   Regarding claim 21, line 13, "the the has", should be --the hash--.

-   Regarding claim 31, lines 1-2, "wherein the authenticating the operably", should
    be --wherein performing the authenticating of the operably--.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   **Claims 1-10, 12-22, 25-34, 36-46 and 50-70** are rejected under 35 U.S.C. 103(a)

as being unpatentable over Hoffberg et al. (USPN 6,640,145), hereinafter referenced as

Hoffberg in view of Cooper et al. (U.S. Publication No. 2002/0029350), hereinafter

referenced as Cooper and in further view of Abdo et al. (US Publication 2002/0080967),

hereinafter referenced as Abdo.

Regarding **claims 1, 25 and 49**, Hoffberg discloses a system, method and

computer program product for securely transforming an audio stream to encoded text,

comprising:

a security core which provides security functions (identifier relevant users;

column 87, lines 32-41),

a plurality of components, comprising at least an audio recording component

(VCR; column 87, line 65 – column 88, line 3 with column 96, lines 15-24) and one or

more transformation components (figure 22, element 2205 with column 103, lines 62-

67),

a security core operating module configured to operate the security core (column

98, lines 59-65);

wherein the components are securely connected to the security core (device

which attaches), such that the security core can vouch for authenticity (for

authentication) of each securely operably connected component (column 99, lines 21-

25); and

wherein the at least one of the securely operably connected audio recording

componet is configured to record an audio stream (VCR) (column 87, line 65 – column

88, line 3 with column 96, lines 15-24), but lacks means for transforming the audio

stream to text and means for securely providing an identification of the securely

operably connected audio and transformation component.

Cooper discloses a web based network, comprising:

wherein the at least one of the securtely connected transformation components is configured to transform the audio stream to a text stream (speech-to-text; column 18, paragraph 0241);

wherein the security core is configured to securely provide, for the text stream, and identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components (digital certificates; column 5, paragraph 0060), to allow immediate identification and authorization of access; and

wherein the security core is configured to detect whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the means for recording and the means for transforming (verify the integrity of the file; column 5, paragraph 0056), to verify the integrity of the file.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein it discloses means for transforming the audio stream to text and means for securely providing an identification of the securely operably connected audio and transformation component, to prevent intrusion by unauthorized third parties (column 5, paragraph 0060) and to identify the certificate as being produced by the certifying authority and to ensure that the certificate has not been altered or forged (column 5, paragraph 0056).

Hoffberg in view of Cooper discloses a system, method and computer program product for securely transforming an audio stream to encoded text, but does not specifically teaching wherein the security core is configured to abort the recording and transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and the transforming of the audio stream.

Abdo teaches a wireless secure device wherein the security core is configured to abort the recording (security mode is switched off without permission being granted by the user; column 1, paragraph 0011) if the audio recording component (VCR; column 1, paragraph 0006) fails to remain operably connected to the security core during the recording (establishes and maintains a secure connection; column 9, paragraph 0086 with column 1, paragraph 0009-0011), to provide a secure connection being highly resistant to coincidental as well as potentially intentional or malicious interference.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg in combination with Cooper's system, method and computer program product such that it teaches detecting whether the audio and transformation component remain operably connected to the security core and if not, aborting the recording or the transformation, to provide a medium of communication that is difficult for unauthorized third party device to eavesdrop on, disrupt, or participate in.

Regarding **claims 2, 26 and 50**, Hoffberg discloses a system, method and computer program product wherein selected ones of the operable connections are

made using one or more buses of the security core (video, audio, home appliances etc.; column 87, lines 38-41 with multimedia input; column 103, lines 45-47).

Regarding **claims 3, 27 and 51**, Hoffberg discloses a system, method and computer program product wherein selected ones of the operable connections are made using a wireless connection between (wireless communication between) respective ones of the components and the security core (column 100, lines 22-24 with column 13, lines 1-6 and lines 20-24).

Regarding **claims 4, 28 and 52**, Hoffberg discloses a system, method and computer program product wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent (DES, "Clipper", elliptic key alogortihms, etc.) which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key (encryption key), and periodic renegotiation of the time-limited key agreement with a new encryption key (column 98, line 59 – column 99, line 9).

An alternate rejection regarding **claims 4, 28 and 52**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but does not specifically disclose SSL data encryption.

Cooper discloses a web based network product wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent (SSL; column 1, paragraph 0013, column 7, paragraph 0089 and column 19, paragraph 0265) which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key (encryption keys) and

periodic renegotiation of the time-limited key agreement with a new encryption key (column 5, paragraphs 0054 and 0059), to facilitate virtual private network (VPN).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein the wireless connections use Secure Sockets Layer (SSL) data encryption, to obtain a secure communication technology that is designed to facilitate VPN.

Regarding **claims 5, 29 and 53**, Hoffberg discloses a system, method and computer program product wherein selected ones of the secure operable connections are provided when the security core is manufactured (column 99, lines 21-25 with lines 53-57).

Regarding **claims 6, 30 and 54**, Hoffberg discloses a system, method and computer program product wherein the security core is configured to authenticate the operably connected component to the security core (column 99, lines 21-25).

Regarding **claims 7, 31 and 55**, Hoffberg discloses a system, method and computer program product wherein the operably connected component is configured to provide a unique identifier (figure 19, lines 1902) of the operably connected component to the security core (column 96, lines 1-11), along with a digital signature of the unique identifier that is created using a private key (private key) of the operably connected component (column 98, lines 59-65); and

the security core is configured to use a public key (public key) that is

cryptographically associated with the private key (private key) to determine authenticity

of the operably connected component (column 98, lines 59-65).

Regarding **claims 8, 32 and 56**, Hoffberg discloses a system, method and

computer program product wherein the component is securely operably connected

after a hardware reset of the component (hardware key), and wherein the hardware

reset is activated by operably connecting of the component (column 99, lines 21-25

with column 108, lines 28-28 and column 115, lines 11-13).

Regarding **claims 9, 33 and 57**, Hoffberg discloses a system, method and

computer program product wherein the unique identifier is securely stored on the

operably connected component (column 99, lines 21-25).

Regarding **claims 10, 34 and 58**, Hoffberg discloses a system, method and

computer program product wherein the security core is authenticated to the operably

connected component (column 99, lines 21-25).

Regarding **claims 12, 36 and 60**, Hoffberg discloses a system, method and

computer program product for providing improved audio compression, but lacks

wherein the security core is configured to mark the text stream as not authenticated if

one or more of the audio recording component and the at least one transformation

component fails to remain operably connected to the security core during the recording

and transforming of the audio stream.

Cooper discloses a web based network product but does not specifically disclose

wherein the security core is configured to mark the text stream as not authenticated if

one or more of the audio recording or transformation component fail to remain operably connected to the security core during the recording and transforming of the audio stream.

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the indication that the original data has been altered is a marking, as taught by Cooper (column 14, paragraph 0182, column 13, paragraph 0171 with column 5, paragraph 0056), to verify the integrity.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product such that the security core is configured to mark the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and transforming of the audio stream, to identify the certificate as being produced by the certifying authority and to ensure that the certificate has not been altered or forged (column 5, paragraph 0056).

Regarding **claims 13, 37 and 61**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but lacks wherein the security core is configured to determine whether the audio recording component and the at least one transformation component have been authenticated to the security core; and

to abort the recording or the transforming if one or more of the audio recording
component and the at least one transformation component has not been authenticated
to the security core.

Cooper discloses a web based network product further wherein the security core
is configured to determine whether the audio recording component and the at least one
transformation component have been authenticated to the security core (verified
biometric data; columns 6-7, paragraph 0075); and

to abort the recording or the transforming if one or more of the audio recording
component and the at least one transformation component has not been authenticated
to the security core (if file has been modified or corrupted, the verification process will
fail; column 5, paragraph 0056 and column 13, paragraph 0173), to verify the integrity
of the file.

Therefore, it would have been obvious to one of ordinary skill in the art at the
time the invention was made to modify Hoffberg's system, method and computer
program product wherein the security core is configured to determine whether the
audio recording component and the at least one transformation component have been
authenticated to the security core and if not, aborting the recording or transforming, to
ensure that the identity of the individual is legally acceptable (columns 6-7, paragraph
0075).

Regarding **claims 14, 38 and 62**, Hoffberg discloses a system, method and
computer program product for providing improved audio compression, but lacks
wherein the security core is configured to determine whether the audio recording

component and the at least one transformation component have been authenticated to

the security core; and

to mark the text stream as not authenticated if one or more of the audio recording

component and the at least one transformation component has not been authenticated

to the security core.

Cooper discloses a web based network product wherein the security core is

configured to determine whether the audio recording component and the at least one

transformation component have been authenticated to the security core verified

biometric data; columns 6-7, paragraph 0075), but does not specifically disclose

marking the text stream as not authenticated if one or more of the audio recording or

transformation component has not been authenticated.

However, it would have been obvious to one of ordinary skill in the art at the time

the invention was made that the indication that the original data has been altered is a

marking, as taught by Cooper (column 14, paragraph 0182, column 13, paragraph

0171 with column 5, paragraph 0056), to verify the integrity.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify Hoffberg's system, method and computer

program product such that it discloses means for determining whether the audio

recording component and the at least one transformation component have been

authenticated to the security core and if not, marking the text stream as not

authenticated if one or more of the audio recording or transformation component has

not been authenticated, to identify the certificate as being produced by certifying

authority and to ensure that the certificate has not been altered or forged (column 5, paragraph 0056).

Regarding **claims 15, 39 and 63**, Hoffberg discloses a system, method and computer program product wherein the security core is configured to digitally notarize the text stream (public/private key; column 98, lines 59-65).

Regarding **claims 16, 40 and 64**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but lacks wherein the security core is configured to provide an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization of the text stream.

Cooper discloses a web based network product wherein the security core is configured to provide an additional data stream that is associated with the text stream (column 20, paragraph 0279), wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream (column 20, paragraph 0271 with column 6, paragraph 0073 and column 5, paragraph 0053), to reduce the possibility that someone would derive a private key from its public key.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein the security core is configured to provide an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream, to

identify the certificate as being produced by certifying authority and to ensure that the

certificate has not been altered or forged (column 5, paragraph 0056).

Regarding **claims 17, 41 and 65,** Hoffberg discloses a system, method and

computer program product for providing improved audio compression, but lacks

wherein the security core is configured to compute, to combine, to sign and to provide

a hash value.

Cooper discloses a web based network product further comprising:

wherein the security core is configured to compute a hash value over the text

stream (hashing algorithm; column 5, paragraph 0055 and column 0073);

to combine the hash value with a unique identifier (unique value) of the audio

recording component and of each of the at least one transformation components,

thereby creating a combination data block (column 5, paragraph 0055 and column 6,

paragraph 0073);

to hash the combination data block (column 5, paragraph 0055 and column 6,

paragraph 0073);

to sign the hashed combination data block (digitally signing message hash) with

a private cryptographic key of the security core (cryptographically), wherein the private

cryptographic key (private key) has a public cryptographic key (public key)

cryptographically associated therewith (column 6, paragraph 0073); and

to provide the digitally signed hashed combination data block (digitally signing

message hash), along with the combination data block, as the digital notarization for

the text stream, wherein the digital notarization cryptographically seals contents

(cryptographically) of the text stream and identifies the audio recording component and each of the at least one transformation components (column 6, paragraph 0073 and column 5, paragraph 0055), for the verification of the signature.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein the security core is configured to compute, to combine, to sign and to provide a hash value, to increase the efficiency of the process of creating and later verifying the signature for larger documents and software files (column 5, paragraph 0055).

Regarding **claims 18, 42 and 66**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but lacks wherein the security core is configured to verify authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and for concluding that the text stream is authentic if the verification succeeds.

Cooper discloses a web based network product wherein the security core is configured to verify authenticity of the text stream (verify the integrity) by a receiver of the text stream and the digital notarization (digitally signed documents), using the public cryptographic key of the security core (public-key cryptography), and for concluding that the text stream is authentic if the verification succeeds (column 5, paragraphs 0054-0056), to verify the integrity.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein the security core is configured to verify authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and for concluding that the text stream is authentic if the verification succeeds, to identify the certificates as being produced by the certifying authority and to ensure that the certificate has not been altered or forged (column 5, paragraph 0056).

Regarding **claims 19, 43 and 67**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but lacks wherein the security core is configured to conclude that the text stream has not been tampered with if the verification succeeds.

Cooper discloses a web based network product wherein the security core is configured to conclude that the text stream has not been tampered with if the verification succeeds (verification process fail; column 5, paragraph 0056), to verify the integrity.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein the security core is configured to conclude that the text stream has not been tampered with if the verification succeeds, to identify the certificates as being produced by the certifying authority and to ensure that the certificate has not been altered or forged (column 5, paragraph 0056).

Regarding **claims 20, 44 and 68**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but lacks wherein the security core is configured to verify authenticity by determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

Cooper discloses a web based network product wherein the security core is configured to verify authenticity by determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof (column 5, paragraph 0055 and column 6, paragraph 0073), to produce a message digest.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hoffberg's system, method and computer program product wherein the security core is configured to verify authenticity by determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof, to increase the efficiency of the process of creating and later verifying the signature for larger documents and software files (column 5, paragraph 0055).

Regarding **claims 21, 45 and 69**, Hoffberg discloses a system, method and computer program product for providing improved audio compression, but lacks

wherein the at least one transformation component comprises an analog to digital transformation component, a speech recognition transformation component and computing, combining and signing the hash value.

Cooper discloses a web based network wherein:

the at least one transformation component comprises an analog to digital transformation component configured to transform the audio stream to a digital stream (sending signals; column 1, paragraph 0013); and

a speech recogntin transformation component (speech-to-text means) configured to convert the digital stream to the text stream (voice recognition means; column 18, paragraph 0241 and columns 6 and 7, paragraph 0075); and

the security core is configured to compute a hash over the text stream (column 5, paragraph 0055);

to combine the hash (hash algorithm) with unique identifiers (unique value) of the audio recording component (column 5, paragraph 0055), the analog-to-digital transformation component (column 1, paragraph 0013), and the speech recognition transformation component (column 18, paragraph 0241 and columns 6 and 7, paragraph 0075); and

digitally signing (digitally signing) the has with unique identifiers using a private cryptographic key (private key)of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith (public key; column 6, paragraph 0073), to verify the integrity of a file.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify Hoffberg's system, method and computer

program product wherein the at least one transformation component comprises an

analog to digital transformation component, a speech recognition transformation

component and computing, combining and signing the hash value, to identify the

certificate as being produced by the certifying authority and to ensure that the

certificate has not been altered or forged (column 5, paragraph 0056).

Regarding **claims 22, 46 and 70**, Hoffberg discloses a system, method and

computer program product for providing improved audio compression but lacks,

comprising an analog-to-digital transformation component, a speech recognition

transformation component, an authenticated speaker specific speech recognition

database, a lexical transformation component and a text compression transformation

component.

Cooper discloses a web based network wherein the at least one transformation

component comprises

the analog-to-digital transformation component configured to transform the audio

stream to a first digital stream (sending signals; column 1, paragraph 0013);

the speech recognition transformation component is configured to convert the

first digital stream to a first encoded text stream (speech-to-text) wherein the speech

recognition transformation component is augmented by the lexical transformation

component and the authenticated speaker specific speech recognition database

(column 18, paragraph 0241 and columns 6 and 7, paragraph 0075); and

the text compression transformation component is configured to compress the

first encoded text stream into the text stream (column 12, paragraph 0153); and

the security core is configured to digitally notarize the text stream by computing

a hash over the text stream (column 5, paragraph 0055);

combining the hash with unique identifiers (column 5, paragraph 0055) of: (1) the

audio recording component (VCR; column 87, line 65 – column 88, line 3 with column

96, lines 15-24); (2) the analog-to-digital transformation component (column 1,

paragraph 0013); (3) the speech recognition transformation component (column 18,

paragraph 0261 with columns 6 and 7, paragraph 0075); (4) the authenticated

speaker-specific speech recognition database (column 18, paragraph 0261 with

columns 6 and 7, paragraph 0075); (5) the text compression transformation component

(column 12, paragraph 0153); and

the security core is configured to sign the hash and unique identifier using a

private cryptographic key of the security core, wherein the private cryptographic key

(private key) has a public cryptographic key cryptographically associated therewith

(public key; column 6, paragraph 0073), to verify the integrity of a file.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify Hoffberg's system, method and computer

program product wherein it comprises an analog-to-digital transformation component, a

speech recognition transformation component, an authenticated speaker specific

speech recognition database, a lexical transformation component and a text

compression transformation component, to identify the certificate as being produced by

the certifying authority and to ensure that the certificate has not been altered or forged

(column 5, paragraph 0056).

6.   **Claims 23-24, 47-48 and 71-72** are rejected under 35 U.S.C. 103(a) as being

unpatentable over Hoffberg in view of Cooper and Abdo, as applied to above, and in

further view of Hoarty et al. (U.S. Patent No. 5,220,420), hereinafter referenced as

Hoarty.

Regarding **claims 23, 47 and 71**, Hoffberg in view of Cooper and Abdo disclose

a system, method and computer program product for securely transforming an audio

stream to encoded text, but lacks wherein the text stream is an ASCII text stream.

Hoarty discloses an interactive home information system wherein the text stream

is an ASCII text stream (column 6, line 66 – column 7, line 4), for textual information.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify Hoffberg in combination with Cooper and Abdo

system, method and computer program product wherein the text stream is an ASCII

text stream, to have the data in an object oriented database, to establish relevant

association (column 7, lines 5-27).

Regarding **claims 24, 48 and 72** Hoffberg in view of Cooper and Abdo disclose a

system, method and computer program product for securely transforming an audio

stream to encoded text, but lacks wherein the text stream is an EBCDIC text stream.

Hoarty discloses an interactive home information system wherein the text stream

is an EBCDIC text stream (column 6, line 66 – column 7, line 4), for textual information.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify Hoffberg in combination with Cooper and Abdo

system, method and computer program product wherein the text stream is an EBCDIC

text stream, to have the data in an object oriented database, to establish relevant

association (column 7, lines 5-27).

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

> Neer (USPN 5,142,560) discloses a wiretap detector and telephone loop monitor

> Diffie et al. (USPN 5,371,794) disclose a method and apparatus for privacy and

   authentication in wireless networks.

8.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

9.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jakieda R Jackson whose telephone number is

571.272.7619. The examiner can normally be reached on Monday through Friday from

7:30 a.m. to 5:00p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Wayne Young can be reached on 571.272.7582. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

JRJ
July 8, 2005

W. R. YOUNG
PRIMARY EXAMINER